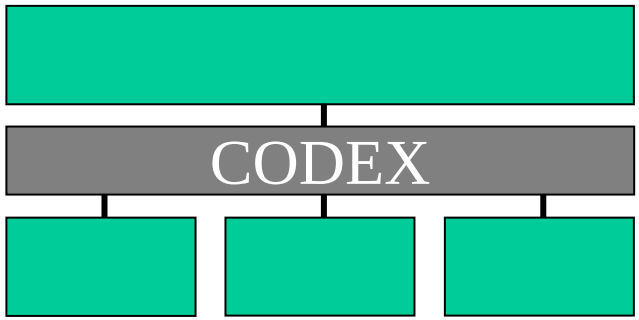
Bibliotheken in Thüringen und Codex – Meta Directory

Jena

Schmalkalden

Weimar



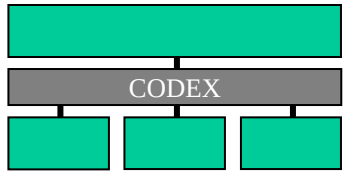
Erfurt

Nordhausen

Ilmenau

Jörg Deutschmann
Universitätsrechenzentrum
Technische Universität Ilmenau

Gliederung

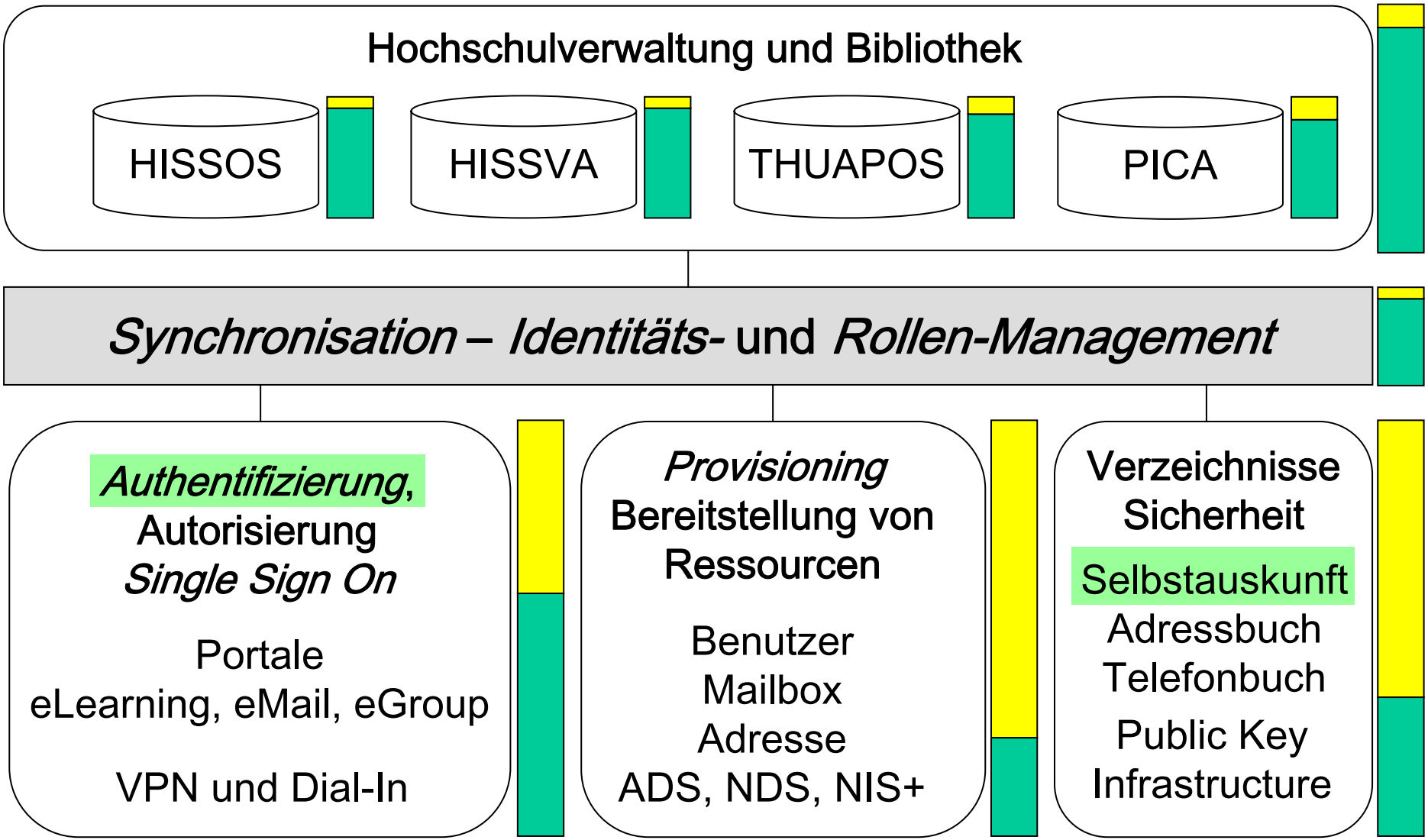


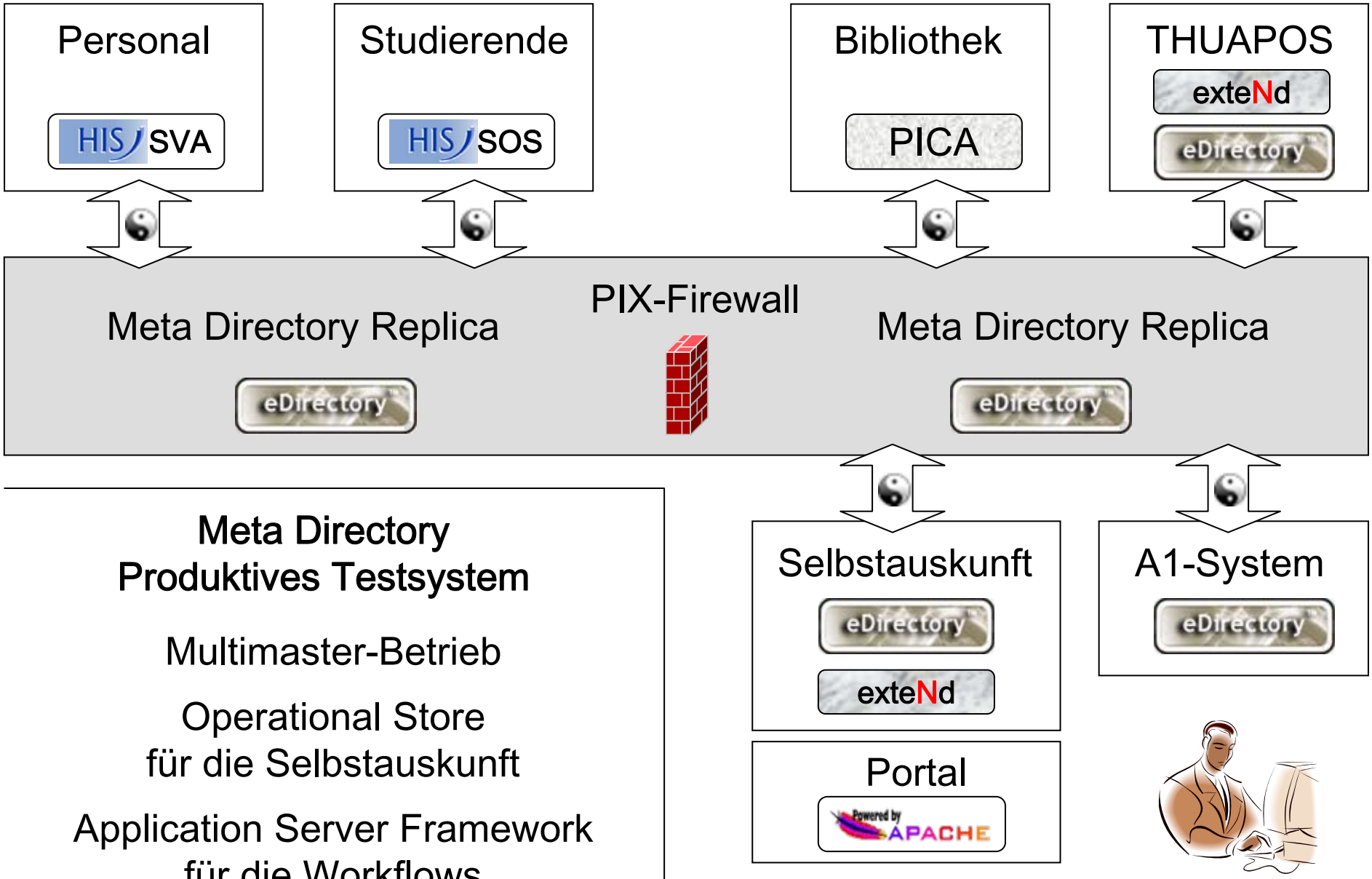
Codex – Meta Directory
Szenario und aktueller Stand
Schemaspezifikation vom 31. Dezember 2005

Konnektivität zu PICA
Technologische Näherung

Weiterentwicklung der Architektur durch föderierte Ansätze
Zusammenfassung und Ausblick

Codex – Meta Directory – Szenario und Stand





Meta Directory
Produktives Testsystem

Multimaster-Betrieb

Operational Store
für die Selbstauskunft

Application Server Framework
für die Workflows

Produktiver Testbetrieb des Meta Directory

- Multimaster-Betrieb
  - Lesender und schreibender Zugriff auf das Meta Directory innerhalb und außerhalb des administrativen Netzes -> nur ein „Loch“ in der PIX
- Operational Store für die Selbstauskunft
  - Keine Anmeldung der Benutzer am Meta Directory
  - Sicherheit durch mehrstufige Indirektion

- Application Server Framework für die Prozesse
  - Prozessunterstützung durch das Meta Directory (ExteNd-Integration in Novell Identity Manager 3)

Spezifikation 31.12.05

thuEduPerson

1

18 Erweiterungen (+ 1 Assoziation)

<>Identifier (cn)
<>StudentNumber
<>LibraryCodeNumber
<>DateOfBirth
<>NameExtension
<>{Academic}Title
<>PostalAddress{Extension}
<>PostalCode
<>PostalCity / Country
<>Salutation
<>DateOfMatriculation
<>SimplePassword
<>Status
<>{Primary}RoleDN

---

8 Standard

eduPerson{Primary}Affiliation
employeeNumber
surname
givenname
organizationalName
mail / uid

N

thuEduRole

13 Erweiterungen (+ 3 Assoz.)

<>RoleType
<>StartDate
<>ExpiryDate
<>CourseOfStudy
<>SemesterOfCourseStudy
<>StudentType
<>Qualification
<>CostAllocation
<>JobType
<>Function
<>House/RoomIdentifier
<>Status

---

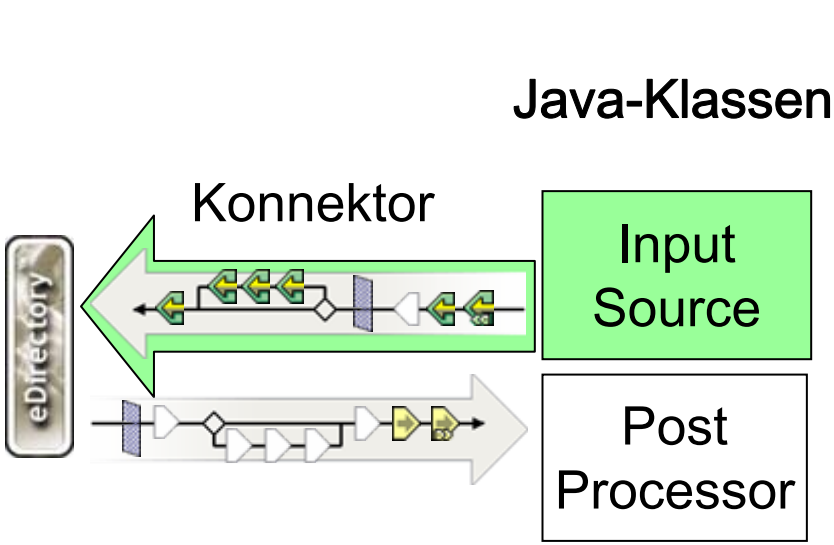
5 Standard

cn
roleOccupant
organizationalUnitName
{Facsimile} Telephone Number

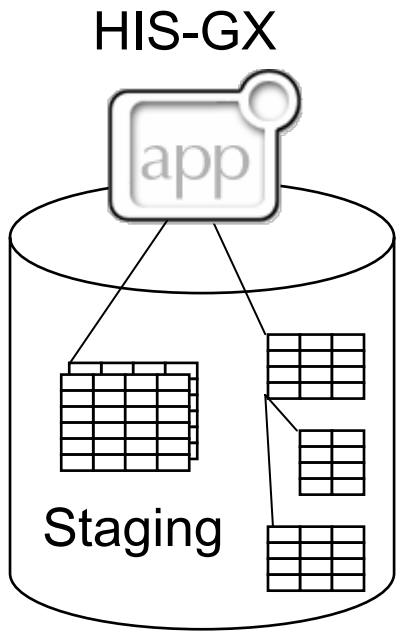
Offene Fragen / Probleme beim PICA-Konnektor

- Organisatorisch-technisch
  - Regeln für die Datenerfassung und Speicherung
    - Titel, akademischer Grad, Namenszusätze etc.
    - Eindeutige Zuordnung von Adressen
  - thoska(+)-Organisation, Datenflüsse
  - Standortbestimmung für externe Bibliotheksbenutzer
  - Einheitliche Belegung der frei definierbaren Felder in LBS4
- Technologisch aufgrund Schema und Dateischnittstelle
  - Preprocessing notwendig

Lösungsansatz am Beispiel Codex-HIS



1. Initial-ADD
2. REF-Management
3. Preprocessing ADD/MOD/DEL
4. Daily Update ADD/MOD/DEL



- Initialbefüllung (ADD-Events) nur für Personen mit Rollen
- Verwaltung von Referenzeinträgen in Java-Zwischenstruktur
- Überprüfung von Einträgen der HIS (Preprocessing)
- Rückfragen in der Datenbank (Call-backs)
- Komplette Überprüfung des Datenbestandes einmal täglich
- Unterstützung von Informix, PostgreSQL und ODBC sowie der HIS-GX Versionen 6, 7 und 8

Authentifizierung, Autorisierung, Rechteverwaltung

- Motivation
  - Eingeschränkter Zugriff, Personalisierte Services
  - Stark differenzierte Lizenzierungen, Konsortialverträge mit kompliziertem Regelwerk
  - Hoher Aufwand für die Benutzerverwaltung
  - Mehrfache Anmeldung / Benutzerkennung, Nutzung nur innerhalb der Einrichtungsgrenzen
- Föderierte Ansätze als Lösungsmöglichkeit
  - Web Services/Security, Liberty Alliance, **Shibboleth**
  - Integration mit SAML v2.0
- AAR – ein Projekt der UB Freiburg / Regensburg

Shibboleth – Begriff (Wikipedia)

Schibboleth (mit Shin: שִׁבֹּלֶת, mit Samech: סִבֹּלֶת) ist ein hebräisches Wort und bedeutet wörtlich 'Getreideähre', wird aber in der Bedeutung von '**Kennwort**' oder '**Codewort**' verwendet. Hintergrund ist eine Stelle aus dem Alten Testament, Buch Richter Kapitel 12 Vers 5ff.
Dort heißt es:

(...) Und wenn ephraimitische Flüchtlinge (kamen und) sagten:
Ich möchte hinüber! fragten ihn die Männer aus Gilead: Bist du ein Ephraimiter? Wenn er nein sagte, forderten sie ihn auf: Sag doch einmal „Schibboleth". Sagte er dann „Sibboleth", weil er es nicht richtig aussprechen konnte, ergriffen sie ihn und machten ihn dort an den Fluten des Jordan nieder. So fielen damals zweiundvierzigtausend Mann am Ephraim.
Ausspracheweisen dienten hier dazu, Personen in die Dichotomie Feind - Nichtfeind zu kategorisieren.

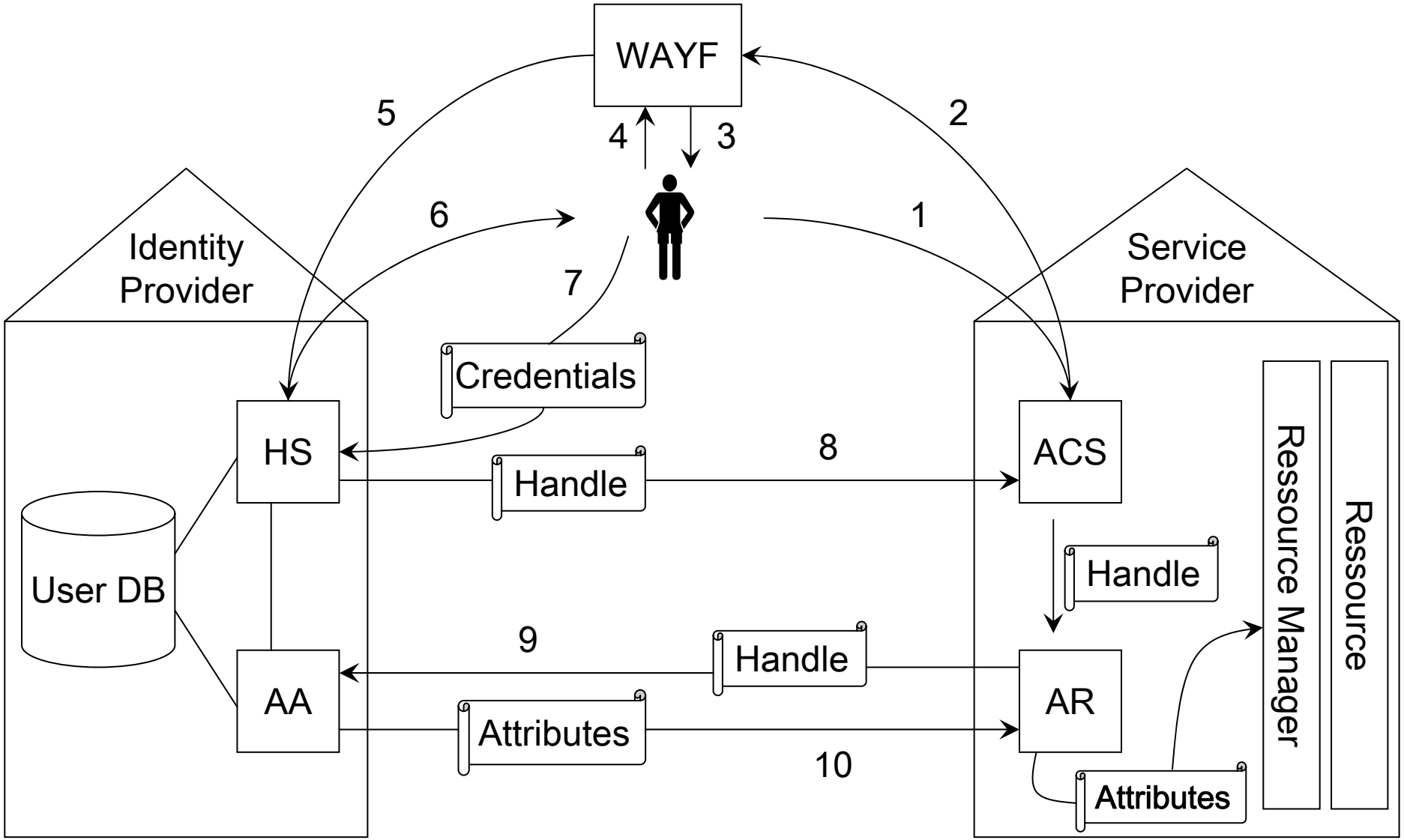
Shibboleth (Internet2, MACE)

- … unterstützt die **autorisierte** Bereitstellung von Web-Ressourcen über Einrichtungsgrenzen hinweg durch Architektur, Regelwerk und Technologie.
- Die Zugriffskontrolle erfolgt über **Attribute** der digitalen Identität des jeweiligen Benutzers.
- Der **Identity Provider** (Origin) einer Einrichtung stellt die Attribute seiner Benutzer dem **Service Provider** (Target) einer anderen Einrichtung zur Verfügung.
- Absolute Grundlage ist, dass sich die Einrichtungen gegenseitig **vertrauen**.
- Zuständig für die Authentifizierung der Benutzer ist der Identity Provider (**Single SignOn**).

Shibboleth – Einführung

- Der Identity Provider (Origin) und der Benutzer (**Privacy**) kontrollieren, welche Attribute dem Service Provider (Target) übermittelt werden.
- Zur Übertragung der Informationen kommt die standardisierte Open Security Assertion Markup Language (OASIS **SAML** v1.1) zum Einsatz.
- Eine erste Menge von Attributen ist durch den **eduPerson**-Standard definiert.
- Das gegenseitige Vertrauen und die anerkannten Regeln sind nicht auf bilaterale Werke beschränkt.
- Entwicklungsziele und Vorteile sind die Vereinfachung des Managements, die Erhöhung der Sicherheit und die Interoperabilität auf der Basis von Standards.

Shibboleth – Architektur (© SWITCH)



Shibboleth – technische Komponenten

- Where Are You From (WAYF)
- Service Provider
  - Assertion* Consumer Service (ACS)
  - Attribute Requester (AR)
    - Attribute Acceptance Policies
  - Ressource Manager
- Identity Provider
  - Handle Service (HS)
  - Attribute Authority (AA)
- Shibboleth Applications = Web-Ressourcen
- Sessions über Cookies und Security Context

*Erklärung, Behauptung, …

Zusammenfassung und Ausblick

- Föderierte Ansätze zeigen einen Weg für den autorisierten Zugriff auf Ressourcen über Einrichtungsgrenzen hinweg auf.
- Bibliotheken haben aufgrund ihrer spezifischen Aufgaben ein besonderes Interesse an diesen Lösungen.
- Codex – Meta Directory befindet sich in der „produktiven Testphase“ und schafft die wichtigste Voraussetzung für einen föderierten Ansatz – Identity Provider.